JCATTファイルフォーマット仕様書

擬似乱数生成関数

２００８年4月１１日

独立行政法人　情報処理推進機構

目 次

1　はじめに

暗号アルゴリズム実装試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する．JCATT が使用するファイルには次のようなものがある．

ファイルの種類

- パラメータファイル (*.par)
  試験項目の設定を記述する．JCATT を用いて作成する．
- リクエストファイル (*.req)
  暗号モジュール開発ベンダに対する要求を記述する．JCATT を用いて作成する．
- Facts ファイル (*.fax)
  テストベクタを記述する．JCATT を用いて作成する．
- レスポンスファイル (*.rsp)
  ベンダからの回答を記述する．リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する．
- 結果ファイル (*.out)
  試験結果を記述する．JCATT を用いて作成する．

これらのファイルの名前は，次の規則に従ってつけること．

ファイル名の規則

- 拡張子は，上記 ( ) 内に指定したものを使用すること．
- 拡張子以外の名前は，試験対象暗号モジュールごとに同じ名称をつけること．
  リクエストファイル (*.req) と Facts ファイル (*.fax) の生成時には，リクエストファイル (*.req) と Facts ファイル (*.fax) に対してパラメータファイル (*.par) と同じ名称を JCATT が自動的につける．
  試験実行時には，同じ名称のレスポンスファイル (*.rsp) と Facts ファイル (*.fax) に対して試験が行われる．また，試験実行時は，結果ファイル (*.out) に対して，Facts ファイル (*.fax) と同じ名称を JCATT が自動的につける．

ファイルフォーマット詳細は次章以降に記述する．各ファイルに共通の規則は次の通りである．

共通規則

- [　] で囲まれた “タグ” の次の行に値を記述する．
- タグは各ファイルフォーマットに記述した順番通りに記述すること．
- レスポンスファイルにおいては,【出力】と記述したタグが，試験対象モジュールが出力するデータを記述する箇所である．
- 半角英数字を用いること．
- タグおよび値は大文字小文字の区別をするので，大文字小文字を含めて正確に記述すること．ただし，数値を 16 進数で記述する場合は，大文字小文字は区別しない．
- 一文字目が ♯(半角) で始まるコメント行を自由に書き込むことができる．
- 平文，暗号文，鍵などのデータの区切り文字は改行 (CR+LF または LF) とする．
- 平文，暗号文，署名，鍵などのデータは 16 進表記とする．
- ビット数，個数などの数値は 10 進表記とする．
- ACSII コードを使用すること．
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)．

2　擬似乱数生成関数

擬似乱数生成関数，PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1，PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1，PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 の暗号アルゴリズム実装試験のためのファイルフォーマットを記述する．この擬似乱数生成関数に対するファイルフォーマットは，`Algorithm Name` の他は同じである．

`Algorithm Name` は，それぞれ下記の通り．

- PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

各表において，試験方法に関する以下の略語を使用する．

- VST: The Variable Seed Test
- MCT: Monte Carlo Test

試験方法の詳細は，暗号アルゴリズム実装試験仕様書を参照のこと．

2.1 パラメータファイル (*.par)

表 1: 擬似乱数生成関数パラメータファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	(暗号名)
	[Function Name]	PRNG
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[Bitlength of XSEED for VST]	VST 用の XSEED のビット長
	[XSEED for VST]	VST 用の擬似乱数生成シード XSEED 値 (optional user input)
	[Bitlength of XKEY for VST]	VST 用の XKEY のビット長
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[Bitlength of XSEED for MCT]	MCT 用の XSEED のビット長
	[XSEED for MCT]	MCT 用の擬似乱数生成シード XSEED 値
	[Bitlength of XKEY for MCT]	MCT 用の XKEY のビット長
	[XKEY for MCT]	MCT 用の擬似乱数生成シード XKEY 値
	[Number of Loop for MCT]	MCT のループの回数

2.2 リクエストファイル (*.req)

表 2: 擬似乱数生成関数リクエストファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	(暗号名)
	[Function Name]	PRNG
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ) [10 進数表記]
	[Bitlength of XSEED for VST]	VST 用の XSEED のビット長 [10 進数表記]
	[XSEED for VST]	VST 用の擬似乱数生成シード XSEED 値 (optional user input) [16 進数表記]
	[Bitlength of XKEY for VST]	VST 用の XKEY のビット長 [10 進数表記]
	[XKEY for VST]	VST 用の擬似乱数生成シード XKEY 値 [16 進数表記]
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ) [10 進数表記]
	[Bitlength of XSEED for MCT]	MCT 用の XSEED のビット長 [10 進数表記]
	[XSEED for MCT]	MCT 用の擬似乱数生成シード XSEED 値 [16 進数表記]
	[Bitlength of XKEY for MCT]	MCT 用の XKEY のビット長 [10 進数表記]
	[XKEY for MCT]	MCT 用の擬似乱数生成シード XKEY 値 [16 進数表記]
	[Number of Loop for MCT]	MCT のループの回数 [10 進数表記]

2.3 Facts ファイル (*.fax)

表 3: 擬似乱数生成関数 Facts ファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	(暗号名)
	[Function Name]	PRNG
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[Bitlength of XSEED for VST]	VST 用の XSEED のビット長
	[XSEED for VST]	VST 用の擬似乱数生成シード XSEED 値 (optional user input)
	[Bitlength of XKEY for VST]	VST 用の XKEY のビット長
	[XKEY for VST]	VST 用の擬似乱数生成シード XKEY 値
	[Random Number for VST]	VST で生成された乱数
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[Bitlength of XSEED for MCT]	MCT 用の XSEED のビット長
	[XSEED for MCT]	MCT 用の擬似乱数生成シード XSEED 値
	[Bitlength of XKEY for MCT]	MCT 用の XKEY のビット長
	[XKEY for MCT]	MCT 用の擬似乱数生成シード XKEY 値
	[Number of Loop for MCT]	MCT のループの回数
	[Random Number for MCT]	MCT で生成された乱数

2.4 レスポンスファイル (*.rsp)

表 4: 擬似乱数生成関数レスポンスファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	(暗号名)
	[Function Name]	PRNG
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ) [10 進数表記]
	[Bitlength of XSEED for VST]	VST 用の XSEED のビット長 [10 進数表記]
	[XSEED for VST]	VST 用の擬似乱数生成シード XSEED 値 (optional user input) [16 進数表記]
	[Bitlength of XKEY for VST]	VST 用の XKEY のビット長 [10 進数表記]
	[XKEY for VST]	VST 用の擬似乱数生成シード XKEY 値 [16 進数表記]
	[Random Number for VST]	【出力】VST で生成された乱数 [16 進数表記]
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ) [10 進数表記]
	[Bitlength of XSEED for MCT]	MCT 用の XSEED のビット長 [10 進数表記]
	[XSEED for MCT]	MCT 用の擬似乱数生成シード XSEED 値 [16 進数表記]
	[Bitlength of XKEY for MCT]	MCT 用の XKEY のビット長 [10 進数表記]
	[XKEY for MCT]	MCT 用の擬似乱数生成シード XKEY 値 [16 進数表記]
	[Number of Loop for MCT]	MCT のループの回数 [10 進数表記]
	[Random Number for MCT]	【出力】MCT で生成された乱数 [16 進数表記]

2.5 結果ファイル (*.out)

表 5: 擬似乱数生成関数結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Function Name]	試験対象機能名
[Results]	試験結果

注

- 試験合格の場合，[Results] に OK と表示される．
- 試験不合格の場合，[Results] に何らかの形式で NG と表示される．また，[Results] には，レスポンスファイル内の不合格となったデータが記述されているタグ名と，そのタグ内の何番目 (No.，#等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし,【出力】と記述したタグが 1 つしかない場合，タグ名は省略することがある．